IJFEAT
INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

FIREWALL TECHNOLOGY IN COMPUTER NETWORK SECURITY

Afsha T. Z. Sayyed[1] ,Vaishnvi G. Banginwar[2], Nikita V. Dehankar[3], Nikita V. Pawar[4]

[1]*Student, computer science and, engineering department J.D.I.E.T, Yavatmal, afshathareen@gmail.com*
[2]*Student, computer science and engineering department, J.D.I.E.T, Yavatmal, vbanginwar02@gmail.com*
[3]*Student, computer science and engineering department J.D.I.E.T, Yavatmal, nikitadehankar15@gmail.com*
[4]*Student, computer science and engineering department J.D.I.E.T, Yavatmal, nikita.pawar005@gmail.com*

ABSTRACT

Firewalls are network devices that enforced an organization's security policy. Since their development, various methods have been used to implement firewalls. These methods filter network traffic at one or more of the seven layers of the IOS (International **O***rganization for* **S***tandardization*)network model, most commonly at the application, transport, network, and data-link levels. Never methods, which have not has been widely and mostly adopted, include protocols normalization and distributed and divided firewalls. Firewalls involve more than the technology to implement them. Specifying a set of filtering rules, known as a policy, is typically complicated and error detected. High-level languages (easy to understand to the firewall) have been developed to simplify the task of correctly defining a firewall's policy. Once a policy rules the firewall has been specified, testing is required to determine if it is correctly implements the policy. Because some data must be able to pass in and out of a firewall, in order for the protected network to be useful, not all attacks can be stopped by firewalls. Some emerging or latest technologies, such as Virtual Private Networks (VPN) and peer-to-peer networking pose new challenges for existing firewall technology.

Keywords*: IP Address, Domain names, Protocols, Ports, Gate way, DMZ*

1. Introduction

A firewall is a network security system designed prevent unauthorized access to or from a private network. Firewalls can be implemented in hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those don't meet the specified security criteria. [2]

1.2 Type of Firewall System

Conceptually, there are three types of firewalls

1. Packet filtering
2. Application-level gateway
3. Circuit-level gateway

1.2.1 Packet Filtering

Network layer firewalls, also known as packet filtering, allows only certain packets to pass through the firewall. Each packet is compared to a set of rules configured for the interface. Rules can be set for incoming and outgoing packets both all. The rules are based on information in the transport protocol header and the IP header. Packet filtering also checks source protocol and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Packet filters also verify source and destination port. The packet filtering firewalls inspects these packets to allow or deny them. [3]

1.2.2 Application-Level Gateway

Application-level firewalls do not just look at the metadata or packets; they also look at the actual data transported. They know how certain protocols work, for example FTP or HTTP. They can then look if the data that is in the packet/metadata is valid (for that protocol). If it is not, it can be rejectedanapplication-level gateway, also called a proxy server, acts as a relay and control of application level traffic. The user contacts the application gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name (IP of the host) of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application level gateway on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further (it can't send to the user) [2]

1.2.3 Circuit-Level Gateway

Circuit level gateways relay TCP connections. The caller connects to a TCP port on the gateway, which some connection are Connects to destination on the other side of the gateway. During the call the gateway's relay program(s) copy the bytes back and forth. The gateway sets two TCP connections, one itself and and another TCP user on an inner host and one between itself and a TCP user on an outside host. The firewall participate TCP connections being made to a host behind it and completes the handshake on behalf of this TCP host. The circuit level getaway security function consists of check which connection will be allowed or not. Once the two connections are established, the gateway usually will not examine the connection and all to access network segment. A typical use of circuit-level gateway is in a particular situation in which the internal users are trusted or not.

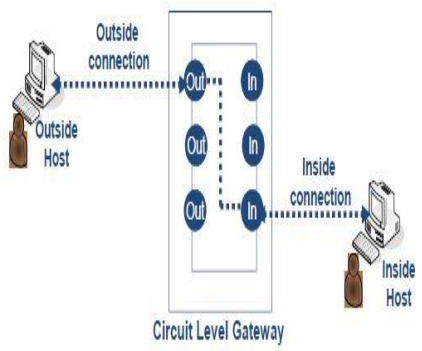

Fig 1.1 Circuit-Level Gateway

2. Demilitarized Zone

The most firewall systems use a demilitarized zone (DMZ) to protect resources and assets of system. A DMZ is a segment or segments (pica of packets) that have a higher security level than that of external segments, but a lower security level than that of internal segments. DMZs are used to grant external users access to public and e-commerce resources such as web side, DNS, and e-mail servers without exposing the systems internal network. A firewall is used to provide the different security-level segmentation among the external, DMZ, and internal resources. Basically, the DMZ acts as a buffer between different areas in a network

2.1 DMZ Rules and Traffic Flow

DMZ are help to enforce security more easily, each areain the firewall system is assigned a security level. This could be something as low, medium, and high, or something more difficult, such as a number between 1 and 50, where 1 is the lowest security level and 50 is the highest. Typically, traffic from a more secure (higher level) layer is permitted to a lower layer, but not vice versa. For traffic to go from a lower level to a higher level, it must be permitted explicitly: In other words, The System must set up a filtering rule that allows this traffic to go from a lower level (1 is low level) to a higher level (50 is high level). If two areas have the same security level, such as medium, the traffic between the two areas is either permitted or not, based on the process that the product uses. The network shown in Figure 2 illustrates how security levels work.

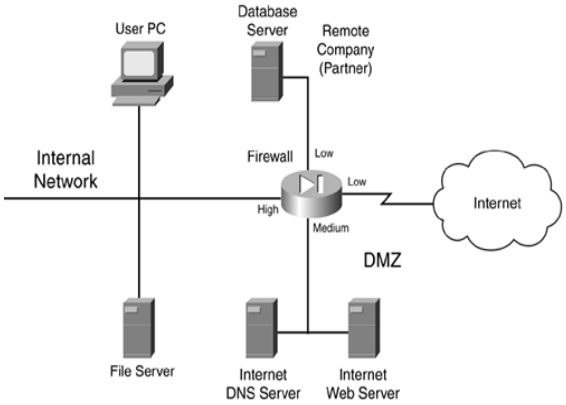

Fig2.1: Security Level Example

In this example, a firewall is used to personal different areas of a network. The firewall has the following interfaces:

- A connection to the Internet, assigned a low security level(assigned to the internet)
- A connection to the DMZ, where public servers are located, assigned a medium security level(median secured only)
- A connection to a remote host company that is working on a some project for them, assigned a low security level(not a good secured)
- A connection to the internal network, assigned a high security level(strong secured connection)

This company has assigned the following rules:

- High- to low-level access: permit
- Low- to high-level access: deny
- Same-level access: deny

Given these rules, the following traffic is allowed automatically to travel through the firewall:

- Internal devices to the DMZ, the remote company, and the Internet
- DMZ devices to the remote company and the Internet[2]

3. Intrusion Detection System Component

The main purpose of the IDS (Intrusion Detection System Component) component is to detect, and possibly prevent, recognition DOS, and unauthorized access attacks. To understand the different kinds of network attacks that The Systems Company is facing, The System need an intimate understanding of the different kinds of traffic flowing through The Systems network, as well as the intentions of this traffic.

Most traffic entering or traversing The Systems network has a valid purpose: to access web pages with HTTP, resolve names to addresses with DNS, send e-mail with SMTP, and so on. However, a small percentage of traffic has malicious (intrusion) intentions. In these cases, a hacker might be executing

a reconnaissance (harm to system) attack to determine what kinds of resources are available in the systems network, and then might execute a DOS attack to affect their level of service or carry out an unauthorized attack to open a back door into The Systems network. An IDS solution should be capable of detecting these kinds of threats. IDS components fall under one of three categories:

- Anomaly-based
- Signature-based

3.1 Anomaly-Based Solutions

Anomaly-based solutions capture traffic (also its call DOS) over a period of time and use this as a reference for what is valid or not valid. These systems then compare new traffic to what is considered to be "normal" and look for anomalies. One limitation of anomaly-positives are bound to happen based solutions is that they tend to generate a lot of false positives. This is because traffic patterns change; if the system do not stay up-to-date on a database of normal traffic flows, false. [2]

4. Conclusion

With a specific case applications of firewall technology in computer network security.is present as the first threshold of network protection, firewall in network security has played an important role. However, despite this excellent choice of firewall performance to achieve the protection of the network, but still in many respects, there is still insufficient.

References

[1] Xin Vue, Wei Chen, Yantao Wang "The Research of Firewall Technology in ComputerNetwork Security" *IEEE* 2009

[2] Vidthya Redya, Dr. K. Shahu Chatrapati, Dr. V. N. Kamalesh" Paper On Types of Firewall and Design Principles*" International Journal of Science and Research (IJSR)* Value (2013): 6.14 | Impact Factor (2015): 6.391

[3] www.Studymafia.Org

[4] William Stalling Data and Compute Communication, Pearson Education

[5] Dr. Ajit Singh, Madhu Pahal, Neeraj Goyat" A Review Paper On Firewall" *International Journal for Research in Applied Science and Technology (IJRASAT)*Vol. 1 Issue II, September 2013

[6] Mr. Sachin Taluja1, Mr. Pradeep Kumar Verma "Network Security Using IP Firewalls"*International Journal of Advanced Research in Computer Science and Software Engineering* Volume 2, Issue 8, August 2012